



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/556,945	04/21/2000	James D. Marks	3042/OG956	6556

7590 02/03/2003

Darby & Darby PC  
805 Third Avenue  
New York, NY 10022

EXAMINER

MORGAN, ROBERT W

ART UNIT	PAPER NUMBER
3626	

3626

DATE MAILED: 02/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.



Art Unit: 3626

## DETAILED ACTION

### *Claim Objections*

1. Amended Claim 31 is objected to because of the following informalities: line 5, the duplicate word “to” should be deleted. Appropriate correction is required.

### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-20, 25-50 and 52-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,731 to Colon et al. in view of U.S. Patent No. 6,171,112 to Clark et al.

As per claim 1, Colon et al. teaches an Internet-networked system with online communication to a computing center from a large number of clinical study investigators at numerous and diverse locations remote from the computing center (see: column 1, lines 36-38). In additions, the system handles automatic assignment and randomization of thousands of participants in a clinical study with respect to care strategies to be administered to the study participants (see: column 1, lines 48-51). Furthermore, the system captures data in its database through appropriate input forms developed for the specific clinical study and the data is stored online and reports are produced in real time to study investigators (reads on “release of at least one of medical and personal information”) and to the sponsor regarding sites that are

Art Unit: 3626

participating, recruitment levels by participating site, patient follow-up, and significant events (see: column 1, lines 64 to column 2, lines 4).

Colon et al. fails to teach the claimed on-line consent to an electronic agreement relating to the release of at least one of medical and personal information.

Clark et al. teaches a method and apparatus for authenticating informed consent for patient that includes providing a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: column 11, lines 66 to column 12, lines 50).

One of ordinary skill in the art at the time the invention was made would have found it obvious to include authenticating informed consent for patient as taught by Clark et al. within the method for managing data used in conducting clinical studies as taught by Colon et al. with the motivation of positively affecting the patient-physician relationship by allowing the physician to accomplish more with each patient in less time (see: Clark et al.: column 3, lines 37-40).

As per claim 2, Clark et al. teaches the electronic agreement is a click wrap consent agreement (see: Fig. 17).

As per claim 3, Clark et al. teaches the claimed generating an electronic survey form to be displayed at the computer terminal, in response to receipt of the individual's consent to the electronic agreement. This limitation is met by the patient selecting the "Agree" button (1771, Fig. 17), which allows a series of questions to be displayed to the patient (see: column 23, lines 62 to column 24, lines 23).

As per claim 4, Colon et al. teaches the claimed electronic survey form comprises at least one of personal and medical related questions. This feature is met by the computer system (17,

Art Unit: 3626

18, 19, Fig. 1) with a screen that brings up a form used for entering patient related data such as identification, demographics and medical conditions and later transmitted to the study management center (10, Fig. 1) as represented by input block (61, Fig. 5) (see: column 6, lines 22-30).

As per claims 5-7, Colon et al and Clark et al. teaches a method of obtaining an informed patient consent during a patient session, which includes the answering of questions by the patient and this data is encrypted and transmitted to a central data facility (see: column 4, lines 31-55). In addition, the data maybe transferred via the Internet, a dedicated local area network, leased private or semi-private data transmission lines using encryption or other secure means (see: Clark et al.: column 10, lines 54-57). Furthermore, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44).

As per claims 8-15, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44). Colon et al. and Clark et al. also teach a method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18). Colon et al. and Clark et al. further teach that transferred data from the data facility (702, Fig. 7) to the Virtual Interactive Teaching and Learning (VITAL) Centers is updated to ensure that the information is up-to-date and accurate

Art Unit: 3626

(see: Clark et al.: column 17, lines 26-30 and Fig. 9). Colon et al. and Clark et al. also teach that only authorized personnel can access the system to protect the integrity of system by minimizing the chance of intentional or inadvertent corruption of patient information (see: Clark et al.: column 12, lines 58-61).

As per claim 16, Colon et al. and Clark et al. teach the claimed generating a certificate to verify transmission between the individual and the secure server. This limitation is met by the patient being asked sign an informed consent electronically and acknowledge of the consent is printed (see: Clark et al.: column 4, lines 19-22). In addition, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44).

As per claim 17, Colon et al. teaches a computer terminal employing a web browser capable of supporting a secure socket layer protocol (see: column 39-41).

As per claim 18, Colon et al. and Clark et al. teach the claimed ensuring decrypted data stored at said secure server is not accessed by unauthorized personnel. This feature is met by the method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18). Clark et al. also teaches that only authorized personnel can access the system to protect the integrity of system by minimizing the chance of intentional or inadvertent corruption of patient information (see: Clark et al.: column 12, lines 58-61). In addition, Colon et al. and Clark et al.

Art Unit: 3626

teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44).

As per claim 19, Colon et al. and Clark et al. teaches the claimed ensuring step comprises at least one of limiting access to said secure server to a minimum number of authorized personnel, identifying as authorized personnel only trustworthy employees, and devising and implementing procedures to ensure that only authorized personnel gain access to the decrypted data. This feature is met by allowing only authorized personnel to access the system to protect the integrity of system by minimizing the chance of intentional or inadvertent corruption of patient information (see: Clark et al.: column 12, lines 58-61). In addition, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44).

As per claim 20, Colon et al. and Clark et al. teach the claimed generating using said secure server an electronic opt-out form to be displayed on the computer terminal to remove the individual's name from a list of consenting individuals. This limitation is met by the eligibility routine, where an determination is made at the time when patient data is submitted, whether the patient qualifies for the clinical study, and if not, a message is communicated to the clinical study investigator's computer (see: Colon et al.: column 2, lines 5-9). In addition, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44). The Examiner considers the message sent to the study investigator's computer regarding eligibility as a form of removing an individual from participating or consenting to the clinical study.

Art Unit: 3626

As per claim 25, Colon et al. teaches an Internet-networked system with online communication to a computing center from a large number of clinical study investigators at numerous and diverse locations remote from the computing center (see: column 1, lines 36-38). In additions, the system handles automatic assignment and randomization of thousands of participants in a clinical study with respect to care strategies to be administered to the study participants (see: column 1, lines 48-51). Furthermore, the system captures data in its database through appropriate input forms developed for the specific clinical study and the data is stored online and reports are produced in real time to study investigators (reads on “release of at least one of medical and personal information”) and to the sponsor regarding sites that are participating, recruitment levels by participating site, patient follow-up, and significant events (see: column 1, lines 64 to column 2, lines 4).

Colon et al. fails to teach the claimed on-line consent to an electronic agreement relating to the release of at least one of medical and personal information.

Clark et al. teaches a method and apparatus for authenticating informed consent for patient that includes providing a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: column 11, lines 66 to column 12, lines 50).

The obviousness of combining the teachings of Colon et al. and Clark et al. are discussed in the rejection of claim 1, and incorporated herein.

As per claims 26-30, they are rejected for the same reasons set forth in claims 2-4 and 6-7 respectively.



Art Unit: 3626

As per claim 31, Colon et al. teaches an Internet-networked system with online communication to a computing center from a large number of clinical study investigators at numerous and diverse locations remote from the computing center (see: column 1, lines 36-38). In additions, the system handles automatic assignment and randomization of thousands of participants in a clinical study with respect to care strategies to be administered to the study participants (see: column 1, lines 48-51). Furthermore, the system captures data in its database through appropriate input forms developed for the specific clinical study and the data is stored online and reports are produced in real time to study investigators (reads on “release of at least one of medical and personal information”) and to the sponsor regarding sites that are participating, recruitment levels by participating site, patient follow-up, and significant events (see: column 1, lines 64 to column 2, lines 4). In addition, Colon et al. teaches the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: column 3, lines 24-44).

Colon et al. fails to teach the claimed on-line consent to an electronic agreement relating to the release of at least one of medical and personal information.

Clark et al. teaches a method and apparatus for authenticating informed consent for patient that includes providing a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: column 11, lines 66 to column 12, lines 50).

The obviousness of combining the teachings of Colon et al. and Clark et al. are discussed in the rejection of claim 1, and incorporated herein.

As per claims 32-33, they are rejected for the same reasons set forth in claims 3-4.

Art Unit: 3626

As per claim 34, A system in accordance with claim 33, wherein said at least one computer terminal is used to enter at least one of personal and medical data in response to the questions in the electronic survey form. This feature is met by the system that captures data in its database through appropriate input forms developed for the specific clinical study and the data is stored online and reports are produced in real time to study investigators and to the sponsor regarding sites that are participating, recruitment levels by participating site, patient follow-up, and significant events (see: column 1, lines 64 to column 2, lines 4).

As per claims 35-42, they are rejected for the same reasons set forth in claims 17, 6 and 8-13, respectively.

As per claim 43, Colon et al. teaches the claimed secure server and central office are a single device at the same location. This limitation is met by the study management center (10, Fig. 1) at a particular geographical site that includes a database host computer (11, Fig. 1) connected via network (12, Fig. 1) to an Internet server (13, Fig. 1) (see: column 2, lines 58-64).

As per claims 44-46, Colon et al. and Clark et al. teach the use of Internet server (13, Fig. 1) used to provide Internet network service to all authorized users (see: Colon et al.: column 3, lines 24-44). Colon et al. and Clark et al. also teach a method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18). Colon et al. and Clark et al. further teach a system that includes a study management center (10, Fig. 1) at a particular geographical site that

Art Unit: 3626

includes a database host computer (11, Fig. 1) connected via network (12, Fig. 1) to an Internet server (13, Fig. 1) (see: Colon et al.: column 2, lines 58-64). In addition, the Internet server (13, Fig. 1) uses Netscape Secure Server software to provide encryption of all material moving to and from the central Internet server (see: Colon et al.: column 3, lines 35-38).

As per claims 47-50 and 52-54, they are rejected for the same reasons set forth in claims 17-20, 7, 20 and 19, respectively.

As per claim 55-56, Colon et al. and Clark et al. teach the on-line recruitment is of candidates for clinical trials and the individual is an end user. This limitation is met by the eligibility routine, where a determination is made regarding the patient submitted data as to whether the patient is qualified for the clinical study. The eligible patients are identified immediately on-line while they are still in the physician's office (see: Colon et al.: column 1, lines 64 to column 2, lines 12). Colon et al. and Clark et al. further teach a method and apparatus for authenticating informed consent for patient that includes providing a means for the patient to input data in the form of answers to questions as well as prompting the patient for electronic signature (see: Clark et al.: column 11, lines 66 to column 12, lines 50).

As per claim 57 and 62, they are rejected for the same reasons set forth in claim 20.

As per claim 58-61, they are rejected for the same reasons set forth in claims 55-56.

4. Claims 21, 24 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,731 to Colon et al. and U.S. Patent No. 6,171,112 to Clark et al. in view of Official Notice.

As per claim 21, Colon et al. and Clark et al. fail to teach the claimed electronic agreement satisfies all federal, state, and local rules, ordinances and regulations.

Art Unit: 3626

However, it is well known in the computer field that electronic agreements or contracts use and follow all federal, state, and local rules, ordinances and regulations. Therefore, it would have been obvious a person of ordinary skill in the art at the time the invention was made to include an electronic agreement that satisfies all federal, state, and local rules, ordinances and regulations with the combined system of Colon et al. and Clark et al. with the motivation of avoiding the any negligent and malpractice litigation caused by not stating and following all federal, state, and local rules, ordinances and regulations.

As per claim 24, Colon et al. and Clark et al. fail to explicitly teach encryption keys stored on a disk kept under physical surveillance.

However, Colon et al. and Clark et al. teach method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18). It is well known in the computer industry for a person to be possession of a disk used to store standard private/public encryption and decryption keys as described by Colon et al. and Clark et al. Therefore, it would have been obvious to a person of ordinary skill in the art the time the invention was made to include storing a encryption keys on a disk kept under physical surveillance with in the system of Colon et al. and Clark et al. with the motivation of preventing unauthorized access to valuable data thereby ensuring the privacy and security of the information.

As per claim 51, it is rejected for the same reasons set forth in claim 21.

Art Unit: 3626

5. Claims 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,731 to Colon et al. and U.S. Patent No. 6,171,112 to Clark et al. in view of U.S. Patent No. 6,272,470 to Teshima.

As per claims 22-23, Colon et al. and Clark et al. teach method and apparatus for authenticating informed consent where transferred patient data (706, Fig. 7) is recorded and stored securely at the data facility (702, Fig. 7) using encryption technology. The encryption ensures maximum protection of patient privacy and the security of the network. Encryption is done using standard private/public key system and a decryption key used to restore the encrypted data to original form (see: Clark et al.: column 17, lines 1-18).

Colon et al. and Clark et al. fail to explicitly teach shareware encryption protocol that is Pretty Good Privacy.

Teshima teaches an electronic clinical recording system that includes encrypting/decrypting software referred to as PGP (Pretty Good Privacy) using public keys (see: column 15, lines 34-41).

One of ordinary skill in the art at the time the invention was made would have found it obvious to include encrypting/decrypting software such as PGP (Pretty Good Privacy) with the system of Colon et al. and Clark et al. with the motivation of preventing unauthorized access to valuable data thereby ensuring the privacy and security of the information.

### *Conclusion*

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Art Unit: 3626

In related art (6,151,581) Kraftson et al. teaches database population and processing by receiving and processing clinical and patient survey information using a hand held computer survey instrument.


In related art (6,105,007) Norris teaches an automatic financial account processing system that includes the consumer signing an electronic signature pad.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert W. Morgan whose telephone number is (703) 605-4441. The examiner can normally be reached on 8:30 a.m. - 5:00 p.m. Mon - Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on (703) 305-9588. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-7687 for regular communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.

RWM  
rwm  
January 29, 2003

  
DINH X. NGUYEN  
PRIMARY EXAMINER

## Recent Statutory Changes to 35 U.S.C. § 102(e)

On November 2, 2002, President Bush signed the 21st Century Department of Justice Appropriations Authorization Act (H.R. 2215) (Pub. L. 107-273, 116 Stat. 1758 (2002)), which further amended 35 U.S.C. § 102(e), as revised by the American Inventors Protection Act of 1999 (AIPA) (Pub. L. 106-113, 113 Stat. 1501 (1999)). The revised provisions in 35 U.S.C. § 102(e) are completely retroactive and effective immediately for all applications being examined or patents being reexamined. Until all of the Office's automated systems are updated to reflect the revised statute, citation to the revised statute in Office actions is provided by this attachment. This attachment also substitutes for any citation of the text of 35 U.S.C. § 102(e), if made, in the attached Office action.

The following is a quotation of the appropriate paragraph of 35 U.S.C. § 102 in view of the AIPA and H.R. 2215 that forms the basis for the rejections under this section made in the attached Office action:

**A person shall be entitled to a patent unless –**

**(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.**

35 U.S.C. § 102(e), as revised by the AIPA and H.R. 2215, applies to all qualifying references, except when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. For such patents, the prior art date is determined under 35 U.S.C. § 102(e) as it existed prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. § 102(e)).

The following is a quotation of the appropriate paragraph of 35 U.S.C. § 102 prior to the amendment by the AIPA that forms the basis for the rejections under this section made in the attached Office action:

**A person shall be entitled to a patent unless –**

**(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.**

For more information on revised 35 U.S.C. § 102(e) visit the USPTO website at [www.uspto.gov](http://www.uspto.gov) or call the Office of Patent Legal Administration at (703) 305-1622.